

What is Claimed is:

1. A random number generation device comprising:

pseudo random number generating means capable of  
outputting random number patterns of a plurality of

5 different pseudo random number sequences;

physical random number generating means for generating  
physical random numbers; and

switching means for switching pseudo random number  
sequences of random numbers that are output by said pseudo  
10 random number generating means on the basis of physical  
random numbers generated by said physical random number  
generating means.

2. A random number generation device according to claim

15 1, wherein:

said pseudo random number generating means having a  
linear shift-register code generator;

said switching means for switching between inverted  
and non-inverted feedback input values to said linear shift-  
20 register code generator on the basis of a physical random  
number generated by said physical random number generating  
means.

3. A random number generation device according to claim

25 1, wherein:

said pseudo random number generating means having a  
linear shift-register code generator;

said switching means for switching between inverted and non-inverted output values from said linear shift-register code generator on the basis of a physical random number generated by said physical random number generating means.  
5

4. A random number generation device according to claim 1, wherein:

said pseudo random number generating means having a linear shift-register code generator and generating a plurality of feedback input values on the basis of different combinations of taps of the linear shift-register code generator;  
10

said switching means for switching, from among said plurality of feedback input values that are generated, the feedback input values to be fed back as input to the linear shift-register code generator on the basis of a physical random number generated by said physical random number generating means.  
15

20

5. A random number generation device according to claim 1, wherein:

said pseudo random number generating means having a linear shift-register code generator for generating a first feedback input value on the basis of a predetermined tap combination and a flip-flop for receiving the first feedback input value, performing bit shifting for a predetermined number of bits in synchronization with said linear shift-  
25

register code generator, and setting the output thereof as a second feedback input value;

said switching means for switching a feedback input value as feedback input to said linear shift-register code generator from among said first or second feedback input value on the basis of a physical random number generated by said physical random number generating means.

6. A random number generation device according to claim 2:

comprising detecting means for detecting a code sequence of said linear shift-register code generator;

wherein, if random numbers of a valid pseudo random number sequence cannot be generated due to said code sequence that was detected, said switching means switch to a pseudo random number sequence other than said pseudo random number sequence.

7. A random number generation device according to claim 2:

comprising detecting means for detecting a code sequence of said linear shift-register code generator;

wherein, if random numbers of a valid pseudo random number sequence cannot be generated due to said code sequence that was detected, at least one bit among bit values of said code sequence is inverted.